REMARKS

Status of Claims

Claim 5 has been amended to correct antecedence. No new matter has been added. No other claim has been amended, added, or deleted. Claims 1-5 remain in the application.

Claim Rejections – 35 USC §112

Claim 5 stands rejected under 35 USC §112, second paragraph, as allegedly being indefinite for using the phrase "the data storage servers" in line 2. Claim 5 has been amended to provide proper antecedent basis. Withdrawal of the rejection of claim 5 is solicited.

Claim Rejections – 35 USC §103(a)

Claims 1 and 5 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Smirnov et al. (US Pub. No. 2003/0097383) in view of Ho (USP 6,148,342), Kesarwani et al. (USP 7,213,258), and Nordman et al. (US Pub. No. 2002/0174364). Also, claims 2-4 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Smirnov et al., Ho, Kesarwani et al., and Nordman et al. in view of "what was well known in the art at the time of the invention." These rejections are respectfully traversed.

The method of independent claim 1 permits the exchange of pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated organizations with which the personal information resides is pseudonymous. In accordance with the method, a unique identification (UID) is assigned to a person having personal information for storage and that person is registered with a pseudonymous proxy server as a user type with associated pseudonym and set of rules that control the person's access to stored data. The person is also provided with a service provider identifier that identifies the person to a service provider. The pseudonymous proxy server with which the person is registered provides both the person's associated pseudonym and the service provider identifier with a random factor and enables the transmission of a message from the person to the service provider. To accomplish the transmission, the pseudonymous proxy server receives the message and, based on the set of rules that control the person's access to stored data, validates a relationship between the person, the service provider and/or a private data owner and

transmits the message to the service provider if the relationship between the person and the service provider is validated. The pseudonymous proxy server also authorizes the person to view the private data owner's actual private data or pseudonyms for the private data based on the set of rules that control the person's access to stored data of the private data owner. The method of the invention thus permits access to data using pseudonyms without learning the identity of the data owner.

The references cited by the examiner do not teach or suggest such a method. In fact, the collective teachings of the cited references fall far short of suggesting the claimed method. Applicant submits that the examiner has merely cited a collection of references purportedly directed to different pieces of the claimed system and has paid no attention to the invention as a whole as required by the obviousness guidelines of the U.S. Patent and Trademark Office. In particular, while the respective references relate to storing and managing data, the references collectively are not directed to different systems and methods for exchanging pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated organizations with which the personal information resides is pseudonymous as claimed. Accordingly, the references taken together do not establish *prima facie* obviousness.

Moreover, contrary to the examiner's allegations, the cited references collectively fail to teach several of the elements of the claims. For example, the examiner alleges that Smirnov et al. teach "registering the person with a pseudonymous proxy server as a user type with associated pseudonym." This is not the case. Smirnov et al. simply teach the use of a "pseudonymity engine." Smirnov et al. say nothing of registering the person as a *user type* with associated pseudonym. Since the person is not assigned as a *user type* as claimed, Smirnov et al. do not teach controlling access to stored data based on a set of rules that limit access to the stored data by user type, for example.

In addition, contrary to the examiner's allegations, Ho does not teach "providing a service provider identifier to the person" where the service provider identifier identifies the person to a service provider. On the contrary, Ho identifies the ID of a user and the ID of a subject but does not provide a "service provider identifier" that identifies the person to a service provider as claimed. As a result, there is no relationship between a pseudonymous

user and a service provider as claimed. Thus, even if Ho would have taught one skilled in the art to modify the Smirnov et al. system to use IDs for the user and the subject, there is no teaching of further providing a "service provider identifier" as claimed.

Furthermore, the examiner alleges that Kesarwani et al. teach the claimed steps of:

> transmitting a message from the person to the service provider through the pseudonymous proxy server, wherein the pseudonymous proxy server receives the message and, based on said set of rules that control the person's access to stored data, validates a relationship between the person, the service provider and/or a private data owner and transmits the message to the service provider if the relationship between the person and the service provider is validated; and
>
> said pseudonymous proxy server authorizing the person to view the private data owner's actual private data or pseudonyms for said private data based on said set of rules that control the person's access to stored data of said private data owner.

This is not the case. Kesarwani et al. instead teach the use of access rules to control a user's access to stored information where Kesarwani et al.'s access rules include, for example, "security access codes, passwords, login IDs, and access information" (column 4, lines 61-63). Kesarwani et al.'s access rules apply to accessing the database – not the private data or pseudonyms for the private data stored in the database. Also, Kesarwani et al. do not validate a relationship "between the person, the service provider and/or a private data owner" and transmitting the message if the relationship is validated.

Finally, while Nordman et al. suggest substituting "randomized pseudonym addresses for the device's real unique address, to confer anonymity upon the user," Nordman et al. do not teach applying a random factor to the person's pseudonym or the service provider identifier as claimed. Indeed, as noted above, the cited references do not teach a service provider identifier, so there can be no teaching of providing a random factor to the service provider identifier as claimed.

Accordingly, contrary to the examiner's allegations, none of the cited references teaches the use of a set of rules to validate the relationship between a pseudonymized person and the service provider for communications after the relationship between the person and the service provider has been validated. Thus, even if the teachings of Smirnov et al., Ho,

Kesarwani et al., and Nordman et al. could somehow have been combined as the examiner alleges, the claimed invention would not have resulted. Withdrawal of the rejection of claims 1-5 is appropriate and is solicited.

Conclusion

In view of the above amendments and remarks, claims 1-5 are believed to be in condition for allowance. A Notice of Allowability is respectfully solicited.

Date: Monday, November 3, 2008

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439